UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/528,161	05/16/2005	Kaisa Nyberg	59643.00600	6511

32294 7590 07/23/2008

SQUIRE, SANDERS & DEMPSEY L.L.P.
8000 TOWERS CRESCENT DRIVE
14TH FLOOR
VIENNA, VA 22182-6212

EXAMINER	
ABYANEH, ALI S	

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
07/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/528,161	NYBERG ET AL.	
	Examiner	Art Unit	
	ALI S. ABYANEH	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 March 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 March 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *17 March 2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1- 20 are presented for examination.

2. Claims 21 and 22 are cancelled.

Information Disclosure Statement PTO-1449

3. The Information Disclosure Statement submitted by applicant on 03-17-2005 has been considered. Please see attached PTO-1449.

Specification

4. The abstract of the discloser is objected to because it includes "means" phrases and it exceeds 150 words.

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The

disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

5. The disclosure is objected to because of the following informalities:

It is not clear in the layout of the specification as where the back ground, summary or detailed description starts and ends. Appropriate correction is required.

The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.

(b) CROSS-REFERENCE TO RELATED APPLICATIONS.

(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.

(d) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC (See 37 CFR 1.52(e)(5) and MPEP 608.05. Computer program listings (37 CFR 1.96(c)), "Sequence Listings" (37 CFR 1.821(c)), and tables having more than 50 pages of text are permitted to be submitted on compact discs.) or REFERENCE TO A "MICROFICHE APPENDIX" (See MPEP

§ 608.05(a). "Microfiche Appendices" were accepted by the Office until March 1, 2001.)

(e) BACKGROUND OF THE INVENTION.

(1) Field of the Invention.

(2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.

(f) BRIEF SUMMARY OF THE INVENTION.

(g) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).

(h) DETAILED DESCRIPTION OF THE INVENTION.

(i) CLAIM OR CLAIMS (commencing on a separate sheet).

(j) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).

(k) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

Claim objections

6. Claim 18-20 are objected to because of the following informalities:

In claims 18-20, phrase "arranged to" is not a positive limitation and does not constitute a limitation in any patentable sense. Examiner suggests the applicant to change the phrase "arranged to" to "configured to".

In the beginning of the claim 20, before "an", remove the letter "**A**". Appropriate correction is required.

Claim Rejections - 35 USC § 101

7. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

8. Claim18 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 18 calls for an "identification means" which does not include any hardware. As such, the claim does not fall within any of the four statutory classes.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. Claims 1-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Green et al. (US Pub No. 2004/00156921 A1).

Regarding claim 1 and 18

Green teaches a method for authenticating a terminal in a communication system, the terminal comprising identification means for applying authentication functions to input data to form response data, and the communication system being arranged to utilise a first authentication protocol for authentication of the terminal, wherein an authentication functionality and the terminal share challenge data, the terminal forms response data and a first key by applying the authentication functions to the challenge data by means of the identification means, and returns the response data to the authentication functionality, and the authentication functionality authenticates the terminal by means of the response data and can apply an authentication function to the challenge data to duplicate the first key (paragraph [0006]; the method comprising;

executing a second authentication protocol wherein the terminal authenticates the identity of a network entity and the terminal and the network entity share a second key for use in securing subsequent communications between the terminal and the network entity (paragraph [0085]-[0086]); and subsequently executing a third authentication protocol by the steps of: sharing challenge data between the network entity and the terminal; forming at the terminal test data by at least applying one of the authentication functions to the challenge data by means of the identification means; transmitting a message comprising terminal authentication data, from the terminal to the network entity; and determining based on the terminal authentication data whether to provide the

terminal with access to a service; wherein in the determining step the terminal is provided with access to the service only if the terminal authentication data equals a predetermined function of at least the test data and the second key (paragraph [0086]).

Regarding claim 19 and 20

Green teaches a communication system comprising a terminal, a network entity and an authentication functionality, the terminal comprising identification means for applying an authentication function to input data to form response data, and the communication system being arranged to utilise a first authentication protocol wherein the terminal authenticates the identity of a network entity and the terminal and the network entity share a key for use in securing subsequent communications between the terminal and the network entity; and the communication system being arranged to perform an authentication method (paragraph [0006]) comprising the steps of: executing a second authentication protocol for authentication of the terminal, wherein an authentication functionality supplies challenge data to the terminal, the terminal forms response data and test data by applying the authentication function to the challenge data by means of the identification means, and returns the response data to the authentication functionality, and the authentication functionality authenticates the terminal by means of the response data; and subsequently executing a third linking protocol by the steps of forming at the terminal secret

session keys by at least applying a predetermined function to the secret test data by means of the shared key established in the first protocol; forming at the network entity secret session keys by at least applying a predetermined function to the secret test data by means of the shared key established in the first protocol; wherein in the secret session keys are used to secure the subsequent communication between the terminal and some network element (paragraph 0085]-[0086]).

Regarding claim 2

Green furthermore teaches a method comprising: forming the test data by applying the authentication function to the challenge data at the authentication functionality; and transmitting the test data from the authentication functionality to the network entity; and wherein the determining step comprises forming network authentication data by applying the predetermined function to the test data and the key at the network entity; and in the determining step the terminal is provided with access to the service only if the terminal authentication data equals the network authentication data (paragraph [0006]).

Regarding claim 3

Green furthermore teaches the method comprises: transmitting the second key from the network entity to the authentication functionality; forming the test data by applying the authentication function to the challenge data at the

authentication functionality; and forming network authentication data by applying the predetermined function to the test data and the key at the authentication functionality (paragraph [0007]).

Regarding claim 4

Green furthermore teaches a method, comprising: transmitting the terminal authentication data from the network entity to the authentication functionality; transmitting from the authentication functionality to the network entity an indication of whether the terminal authentication data equals the network authentication data; and wherein in the determining step the terminal is provided with access to the service only if the indication is that the terminal authentication data equals the network authentication data (paragraph [0086]).

Regarding claim 5

Green furthermore teaches a method, comprising: transmitting the network authentication data from the authentication functionality to the network entity; and wherein in the determining step the terminal is provided with access to the service only if the indication is that the terminal authentication data equals the network authentication data (paragraph [0086]).

Regarding claim 6

Green furthermore teaches a method, wherein the terminal authentication data is formed as a cryptographic checksum (paragraph [0006]).

Regarding claim 7

Green furthermore teaches a method, wherein the network entity is co-located with the authentication functionality (paragraph [0005]).

Regarding claim 8 and 9

Green furthermore teaches a method, wherein authentication means is an identity module of the terminal; and wherein the identity module is user-removable from the terminal (paragraph [0006]).

Regarding claim 10

Green furthermore teaches a method, wherein the identity module is a SIM or a USIM (paragraph [0003]).

Regarding claim 11 and 12

Green furthermore teaches a method, wherein the first authentication protocol is the AKA protocol or any protocol of the EAP family; and wherein the first authentication protocol is the AKA protocol or any protocol of the EAP family,

and wherein the test data includes one or both of the AKA IK value or the AKA CK value. (Paragraph [0006]).

Regarding claim 13-15

Green furthermore teaches a method, wherein the authentication means stores a code and the authentication function comprises applying a cryptographic transformation to the code and the input data; wherein the second authentication protocol is the PIC, the PEAP protocol or the EAP-TTLS protocol; and wherein the challenge data and the response data are formed according to the EAP protocol (Paragraph [0006]).

Regarding claim 16

Green furthermore teaches a method, wherein the said message is a dedicated authentication message (paragraph [0013]).

Regarding claim 17

Green furthermore teaches a method, wherein the predetermined function is used for derivation of a session key to be used for encryption and/or authentication of communications between the terminal and the network entity (paragraph [0006]).

References Cited, Not Used

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

1. U.S. Patent No. 6,760,444 B1

This reference relates to a method and apparatus for authenticating a mobile node.

2. U.S Patent No. 7,231,521 B2

This reference relates to authentication and key exchange methods in wireless LAN network.

3. U.S. Publication No. 2002/0154776 A1

This reference relates to encrypted communications, including air interface communication within secure communication systems.

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ali Abyaneh whose telephone number is (571) 272-7961. The examiner can normally be reached on Monday-Friday from (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone numbers for the organization where this application or proceeding is assigned as (571) 273-8300 Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Ali S Abyaneh/
Examiner, Art Unit 2137
07-17-2008

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137